

Tech

Chaos and hackers stalk investors on cryptocurrency exchanges

Poor security and lack of investor protections plague exchanges.

Steve Stecklow, Alexandra Harney, Anna Irrera and Jemima Kelly, Reuters / 2 October 2017 15:50

 No comments so far



When cryptocurrency exchanges collapse, investors have little chance of recovering any money. Picture: Shutterstock

Dan Wasyluk discovered the hard way that trading cryptocurrencies such as bitcoin happens in an online Wild West where sheriffs are largely absent.

Wasyluk and his colleagues raised bitcoins for a new tech venture and lodged them in escrow at a company running a cryptocurrency exchange called Moolah. Just months later the exchange collapsed; the man behind it is now awaiting trial in Britain on fraud and money-laundering charges. He has pleaded not guilty.

Wasyluk's project lost 750 bitcoins, currently worth about \$3 million, and he believes he stands little chance of recovering any money.

"It really was kind of a kneecapping of the project," said Wasyluk of the collapse three years ago.

"If you are starting an exchange and you lose clients' money, you or your company should be 100% accountable for that loss. And right now there is nothing like that in place."

Cryptocurrencies were supposed to offer a secure, digital way to conduct financial transactions, but they have been dogged by doubts. Concerns have largely focused on their astronomical gains in value and the likelihood of painful price crashes. Equally perilous, though, are the exchanges where virtual currencies are bought, sold and stored. These exchanges, which match buyers and sellers and sometimes hold traders' funds, have become magnets for fraud and mires of technological dysfunction, a Reuters examination shows, posing an underappreciated risk to anyone who trades digital coins.

Huge sums are at stake. As the prices of bitcoin and other virtual currencies have soared this year – bitcoin has quadrupled – legions of investors and speculators have turned to online exchanges. Billions of dollars' worth of bitcoins and other cryptocurrencies – which aren't backed by any governments or central banks – are now traded on exchanges every day.

"These are new assets. No one really knows what to make of them," said David L. Yermack, chairman of the finance department at New York University's Stern School of Business.

"If you're a consumer, there's nothing to protect you."

Regulators and governments are still debating how to handle cryptocurrencies, and Yermack says the US Congress will ultimately have to take action.

Some of the freewheeling exchanges are plagued with poor security and lack investor protections common in more regulated financial markets, Reuters found. Some Chinese exchanges have falsely inflated their trading volume to lure new customers, according to former employees.

There have been at least three dozen heists of cryptocurrency exchanges since 2011; many of the hacked exchanges later shut down. More than 980 000 bitcoins have been stolen, which today would be worth about \$4 billion. Few have been recovered. Burned investors have been left at the mercy of exchanges as to whether they will receive any compensation.

Nearly 25 000 customers of Mt. Gox, once the world's largest bitcoin exchange, are still waiting for compensation more than three years after its collapse into bankruptcy in Japan. The exchange said it lost about 650 000 bitcoins. Claims approved by the bankruptcy trustee total more than \$400 million.

In July, a federal judge in Florida ordered Paul Vernon, the operator of a collapsed US exchange called Cryptsy, to pay \$8.2 million to customers after he failed to respond to a class-action lawsuit. The judge ruled that 11 325 bitcoins had been stolen but did not identify the thief. "This is no different than bank robbers in the Old West," said David C. Silver, one of the plaintiffs' attorneys. "Cryptocurrency is just a new front." Vernon could not be reached for comment.

Another challenge for traders: government intervention. This month, Chinese authorities ordered some mainland Chinese cryptocurrency exchanges to stop trading. The order, however, did not apply to exchanges based in Hong Kong or outside China, including those affiliated with mainland Chinese exchanges.

So-called "flash crashes" – when cryptocurrencies suddenly plummet in value – are also a threat. Unlike regulated US stock exchanges, cryptocurrency exchanges aren't required to have circuit breakers in place to halt trading during wild price swings. Digital coin exchanges are also frequently under assault by hackers, resulting in down times that can sideline traders at critical moments.

On May 7, traders on a US exchange called Kraken lost more than \$5 million when it came under attack and couldn't be accessed, according to a class-action lawsuit filed in Florida. During the incident, the suit alleges, the exchange's price of a cryptocurrency called ether fell more than 70% and the traders' leveraged positions were liquidated. They received no compensation. The exchange declined to comment on the lawsuit. In a court filing, it asked for the case to be dismissed and said the claims should be decided by arbitration.

Another two flash crashes occurred this year on the US exchange GDAX. The exchange said it compensated traders who lost money.

Not surprisingly, many banks are leery of cryptocurrency exchanges and some have refused to deal with them. At a bank investor conference this month in New York, Jamie Dimon, chief executive of JPMorgan Chase & Co, called bitcoin "a fraud" and predicted it will "blow up."

Boycotts by banks can make it impossible at times for exchanges to process wire transfers that allow customers to buy or sell cryptocurrencies with traditional currencies, such as dollars or euros. In March, Wells Fargo stopped processing wire transfers for an exchange called Bitfinex, leaving

customers unable to transfer US dollars out of their accounts, except through special arrangement with the exchange's lawyer. Wells Fargo declined to comment.

Dealing with the banks "is a constant and ongoing challenge," said Bitfinex chief executive Jean Louis van der Velde. "Citizens and businesses being treated like criminals when they are not, including myself." He declined to say which banks Bitfinex is now using.

In part, banks say they are concerned about the due diligence cryptocurrency exchanges do on their customers to guard against money laundering, criminal activity and sanctions violations. While regulators require banks to verify who their customers are, some cryptocurrency trading platforms have performed minimal checks, Reuters found.

Internal customer records reviewed by Reuters from the BTCChina exchange, which has an office in Shanghai but is stopping trading at the end of this month, show that in the fall of 2015, 63 customers said they were from Iran and another nine said they were from North Korea – countries under US sanctions.

Americans are generally prohibited from conducting financial transactions with individuals in Iran and North Korea. Statements on BTCChina's website from 2013 and 2014 identify Bobby Lee, who holds American citizenship, as its chief executive and co-founder. Lee is currently CEO of BTCC, a separate Cayman Islands-registered cryptocurrency exchange company, according to a spokesman for the exchanges.

The spokesman did not respond to repeated questions from Reuters as to Lee's current role at BTCChina, and Lee did not comment on the issue. The spokesman said that BTCChina complies with Chinese law and "is run by a Chinese citizen, and its legal representative is also a Chinese citizen."

The spokesman originally said the exchange had "significantly strengthened" its compliance processes over the last two years, including "banning registrations from sanctioned countries such as Iran and North Korea. Our system still has some inactivated accounts from some sanctioned countries for audit and logging purposes." He said "most" of those accounts had never been used to trade.

He later said that BTCChina has never had any North Korean customers and "has had only one Iranian customer." The Iranian used a bank account in China, not Iran, "therefore all of that customer's transactions on our trading platform did not violate" US sanctions, the spokesman said. He said "BTCC has never had and does not have any North Korean or Iranian customers."

The US Treasury Department's Office of Foreign Assets Control in Washington, which enforces economic and trade sanctions, declined to comment.

In mid-2016, the Chinese exchange hired a compliance analyst to help monitor any suspicious activity on the trading platform. It selected Constance Yuan, then 23 years old, who told Reuters she had no prior formal training in compliance. On her LinkedIn page, she listed her title as "Senior compliance manager."

"I was a bit surprised," Yuan said of her hiring. "I felt I had no experience, and it was a pretty big responsibility." She said lawyers taught her on the job, which she recently left.

The spokesman for BTCChina told Reuters it has had a vice president in charge of compliance on its staff since 2013 and that person helped to develop a "robust" system to verify customers' identities.

Mickey Mouse identities

Bitcoin, the first digital currency to gain widespread acceptance, sprang up during the financial crisis about nine years ago. Its attraction, early proponents maintained, was that it offered a way to bypass banks and governments, and to conduct financial transactions more cheaply. Every transaction is validated and recorded on a public ledger called a blockchain that is maintained by a network of computers. While anonymous, the individual transactions are available for all to see on the internet. They are secured by cryptography, the computerised encoding and decoding of data.

Mike Hearn, an early bitcoin developer, said bitcoin was initially viewed more as a hobby than a serious alternative to traditional money. "People didn't really think it could take off and get big," he said. "It was a thought experiment that happened to have some code."

Though bitcoin turned out to generate huge attention and media coverage, it is still not widely used by ordinary consumers. Few retailers accept it, and processing transactions on the blockchain remains much slower than payment card networks, despite some recent technical changes.

The computer maker Dell, which announced in 2014 that it would accept bitcoin payments, has stopped "due to low usage," a spokeswoman said. At the US online retailer Overstock.com, only a fraction of 1% of sales are transacted in bitcoins, according to the company.

"Most of the cryptocurrencies right now are more commodities than currency," said Dan Schulman, chief executive of payments company PayPal. "You trade them based on what you think will happen to their value. They're not really accepted by many merchants as a currency."

Instead, cryptocurrencies have proved attractive to those seeking anonymity.

Poloniex, a US exchange, has allowed some customers to trade cryptocurrencies and withdraw up to \$2 000 worth of digital coins a day by providing only a name, an email address and a country, Reuters found. In a statement, Poloniex said it “has spent considerable resources developing a culture of compliance and has systems in place to prevent users from abusing the platform.”

The exchange isn’t allowed to accept New York residents as customers because it lacks a state license to operate a cryptocurrency exchange. But Reuters interviewed two New York residents who had claimed that they lived elsewhere and were able to trade on Poloniex. A Poloniex spokesman said, “Any NY resident who submits false profile information in order to trade on our platform is in breach of our terms of service.”

Informed by Reuters of the trading on Poloniex by New York residents, the state’s Department of Financial Services said it would “take appropriate action.” In a statement, the department said: “As New York’s regulator of cryptocurrency, DFS will not tolerate any activity by unlicensed operators who attempt to conduct business in the state.”

In June, a former US federal prosecutor testified before Congress that criminals – including distributors of malicious code called ransomware, “large drug kingpins and serial fraudsters” – were increasingly using unregulated foreign exchanges that don’t verify their customers.

“Criminals can open anonymous accounts, or accounts with phony names to fly under the radar of law enforcement,” Kathryn Haun, a former assistant US attorney, said at a congressional hearing. “Thus, we have received ‘Mickey Mouse’ who resides at ‘123 Main Street’ in subpoena returns.”

Haun left the Justice Department in May and joined the board of Coinbase, which runs the GDAX exchange. She told Reuters she was impressed with Coinbase’s team and vision. A class-action lawsuit was filed last year against Coinbase on behalf of customers of the collapsed Cryptsy exchange. It claims that Coinbase converted bitcoins allegedly stolen from Cryptsy into about \$8.2 million that was then withdrawn. Haun and Coinbase declined to comment on the case; in a court filing, Coinbase denied any wrongdoing.

In July, US authorities shut down the website of the BTC-e exchange, one of the world’s largest, and ordered it to pay a \$110 million fine. The Treasury Department said it had “facilitated transactions involving ransomware, computer hacking, identity theft, tax refund fraud schemes, public corruption, and drug trafficking.”

BTC-e required only a username, password and email address to open an account, authorities said.

Reuters was unable to contact BTC-e, whose base of operations was unclear, though it continues to have a website using a New Zealand domain name. It now forwards to a new exchange called WEX, which didn't respond to a request for comment.

Fake volume

One of the criteria traders say they use to select an exchange is trading volume. The more trades an exchange handles, the faster buyers and sellers can be matched.

From about early 2014 until late January this year, Chinese exchanges accounted for about 90% of global bitcoin trading volume, according to the website bitcoinity.org, which collates trading data reported by exchanges.

Some of that high volume occurred because traders were attracted by the fact that these exchanges at that time charged no transaction fees. But some of the volume was fake, six former employees at two Chinese exchanges told Reuters. Artificially pumped-up volumes in China could have affected the often volatile price of bitcoin, because investors elsewhere monitor and respond to the activity.

One exchange, OKCoin, inflated volumes through so-called wash trades, repeatedly trading nominal amounts of bitcoin back and forth between accounts, two former executives said. The transactions were logged on the exchanges but not recorded on the blockchain, according to a former employee.

Zane Tackett, who held several positions at OKCoin from 2014 to 2015 including international operations manager, said he resigned partly out of concern about its fake volumes. "The motivation is to seem larger than their competition," he said.

Changpeng Zhao, a former chief technical officer at OKCoin, stated on the website reddit.com in May 2015 that OKCoin used bots that "are designed to pump up volumes." In a response to the post, OKCoin said: "OKCoin does not need to have any fake volume."

In a statement to Reuters, OKCoin said it "never artificially inflated trading volume."

Four former employees at BTCChina, including one of its co-founders, said the exchange had also engaged in faking its trading volumes. A spokesman for the exchange said it "has never faked its trading volumes."

The Chinese exchanges' sky-high volumes appear to have caught the attention of the People's Bank of China. After a series of inspections by the central bank, Chinese exchanges in January began charging trading fees – as exchanges elsewhere typically do – and volumes in China plummeted.

"A deceptive market is not a healthy market," said Xiaoyu Huang, a co-founder of BTCChina, who said that the exchange had faked some of its volume. "And, in fact, it was the fake volumes that made the government mistakenly believe that the Chinese market accounted for so much of the

global trading volume, and caused the government to supervise bitcoin in China so forcefully.” Huang said he had left the company in part over a disagreement over its direction.

The spokesman for BTCChina said “the Chinese government’s scrutiny into bitcoin exchanges earlier this year was because of a dramatic increase in bitcoin’s price.” China’s central bank declined to answer questions.

Under attack

Exchanges are frequently targeted by hackers, causing additional problems for investors.

Walle Wei, a Chinese trader based in Guangxi in southern China, said he was trading futures in bitcoin and a cryptocurrency called litecoin on OKCoin.com on July 10 2015. Betting that the litecoin price, then about \$4, would rise, he bought contracts for long positions using borrowed money. This meant that he only had to put down 10% to trade. Trading with that much leverage meant that a small move in the price could either wipe out his positions or greatly magnify his gains.

Instead of rising as Wei had hoped, litecoin’s price began falling and OKCoin’s website slowed down, Wei said. He was unable to buy or sell. When he regained access to his account, his contracts had been liquidated. He said he lost 3 136 litecoins, then worth about \$12 500.

OKCoin announced on its blog that it had been a victim of “large scale” attacks by hackers who flooded its websites with traffic, preventing some users from accessing their accounts.

On July 13, Wei suffered a second, similar event with bitcoin. He said the exchange’s website became inaccessible, his contracts were liquidated and he lost 57.9 bitcoins, then worth about \$16 900.

Wei said he complained and OKCoin covered 15% of his bitcoin losses, waived one month’s worth of trading fees and gave him a mobile phone charger. He said he also filed complaints with police and five government agencies, including the central bank and the China Securities Regulatory Commission (CSRC). Most ignored his complaints, he said, and those that replied told him his problem didn’t fall under their jurisdiction.

“They said to find the relevant department. But I don’t know what other relevant government departments there are,” he said.

A person close to the CSRC said cryptocurrency exchanges fall under the purview of the central bank, which declined to answer questions.

In a written response, OKCoin said it had invested heavily in guarding against attacks and there was no precedent for multinational corporations to compensate users for service interruptions. “All trading’s profit or loss should be solely borne by the users,” OKCoin said. To open an account,

customers must agree to terms of service that absolve the company of liability for losses from “hacker attacks” and “computer virus intrusion or attack.”

Inaccessible websites aren't the only way investors can lose money on exchanges. In February, a hedge fund called GABI, based in Jersey, bought a futures contract on OKCoin's Hong Kong exchange, betting the price of bitcoin would rise. But the contract was liquidated soon afterwards when another investor placed a giant bet the other way that dwarfed it.

In regulated exchanges, such as the Chicago Mercantile Exchange, there are limits to the size of futures contracts to prevent one trader from dominating the market. That's not the case on some cryptocurrency exchanges.

In its online February newsletter, the hedge fund's manager called the incident “clear market manipulation.” He said he questioned OKCoin about it: “They confirmed to us that there were no position limits whatsoever and that people were free to do whatever they wanted in their ‘happy trading environment’ (yes, they used those actual words).”

The February bitcoin contract cost the hedge fund between \$400 000 and \$500 000, according to a person familiar with the matter.

OKCoin said the “two customers traded fairly” and “there is no regulation restricting the trading strategy.” Hong Kong's Securities and Futures Commission declined to comment.

‘An absolute disgrace’

In the past 15 months, Bitfinex, one of the world's largest cryptocurrency exchanges, was fined by a US regulator, lost \$72 million worth of bitcoins to hackers and was cut off by Wells Fargo, one of America's biggest banks.

Bitfinex was set up four years ago. Its hundreds of thousands of clients include banks, investment funds and other cryptocurrency exchanges, according to van der Velde, its CEO and co-founder, and its lawyer.

It has no head office, is owned by a British Virgin Islands company and is managed by three executives who live in Hong Kong, the United States and Europe. Besides its Dutch chief executive, they include chief financial officer Giancarlo Devasini, who is Italian, and Chief Strategy Officer Philip Potter, an American who once worked at Morgan Stanley.

In June 2016, the US Commodities Futures Trading Commission fined Bitfinex \$75 000 for offering “illegal” cryptocurrency transactions and failing to register as a futures commission merchant.

“We were happy with the terms of the settlement,” said Stuart Hoegner, Bitfinex's general counsel.

In August 2016, hackers stole 119 756 bitcoins from Bitfinex.

As customers and others went online to vent their anger – “@bitfinex is an absolute DISGRACE to the #bitcoin community and needs to go,” one Twitter user wrote – Bitfinex executives weighed their options. Convinced they couldn’t get a bank loan and lacking insurance, they decided to reduce their customers’ balances by 36 %, regardless of whether the investor accounts had been hacked – a technique known as the “socialization” of losses.

The exchange distributed IOUs in the form of digital tokens, which could be traded on Bitfinex. Some customers converted the tokens into equity in the company that operates the exchange. Although the exchange later redeemed the tokens in full, some customers had already sold them at a loss.

In an interview, van der Velde expressed regret for the hack. But he defended his firm’s response. “I felt – and I still feel – terrible for those people who lost their money,” he said.

He declined to discuss how the hack happened, citing an ongoing police investigation. “We took responsibility. How many financial institutions in the past can you find that say within a very short time, ‘We are good for that loss, and we issue an IOU for that’? Please find me one.”

He also said Bitfinex has acted transparently, has rigorous know-your-customer procedures and cooperates with law enforcement agencies.

Despite its numerous challenges, van der Velde said Bitfinex is now handling about \$12 billion in trades a month and is “very profitable.” Last year, the exchange said it expected to make a \$20 million profit in 2017. Despite all the Wild West problems besetting cryptocurrencies, van der Velde predicted the final amount will turn out to be even higher.

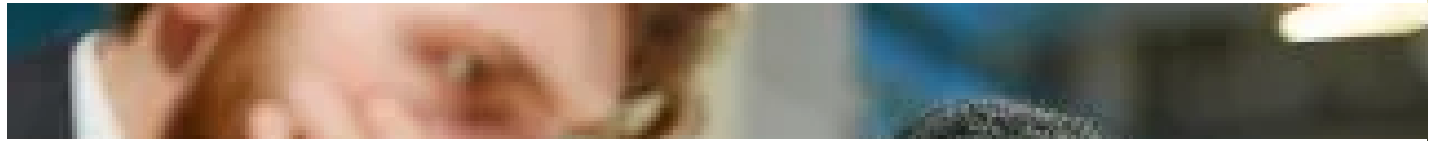
LATEST STORIES

er plans listeria class action against Tiger Brands

SA rights lawyer plans listeria class action against Tiger Brands

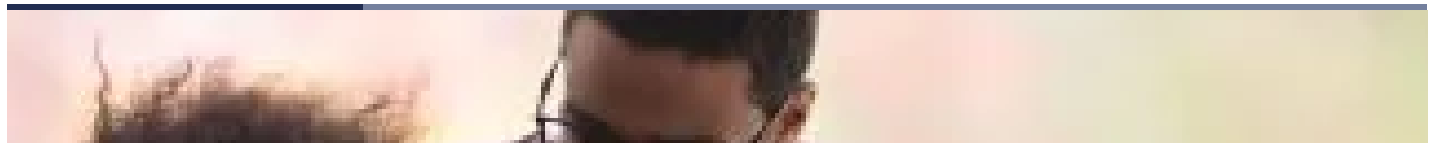


Here's what every live-in couple should know about sharing expenses

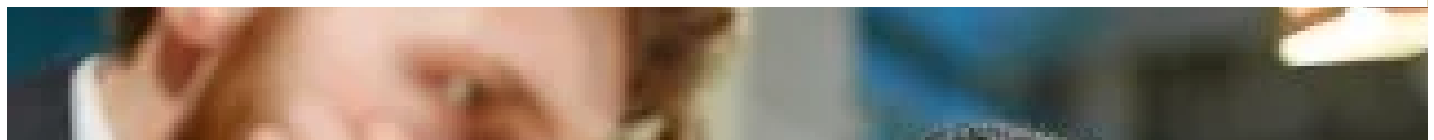


It takes a nation to raise a child

LATEST OPINION



Here's what every live-in couple should know about sharing expenses



It takes a nation to raise a child

h firms trying to get you hooked on bitcoin

Beware fintech firms trying to get you hooked on bitcoin

